G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES

Accurate Detection.
Real Time Response.
Faster Recovery.

Planned list of Test Cases for Smart Medic Platform

STRYKER, INDIA

stryker

April 12th, 2022

Warning: THIS DOCUMENT MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE AREA WHEN NOT IN USE. G' SECURE LABS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT AFTER DELIVERY TO THE ORGANIZATION NAMED HEREIN. IT IS THE ORGANIZATION'S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.

THIS REPORT CONTAINS PROPRIETARY INFORMATION THAT IS NOT TO BE SHARED, COPIED, DISCLOSED OR OTHERWISE DIVULGED WITHOUT THE EXPRESS WRITTEN CONSENT OF G' SECURE LABS OR THEIR DESIGNATED REPRESENTATIVE. USE OF THIS REPORTING FORMAT BY OTHER THAN G' SECURE LABS OR ITS SUBSIDIARIES IS STRICTLY PROHIBITED AND MAY BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

Disclaimer: THE RECOMMENDATIONS CONTAINED IN THIS REPORT ARE BASED ON INDUSTRY STANDARD "BEST PRACTICES". BEST PRACTICES ARE, BY NECESSITY, GENERIC IN NATURE AND MAY NOT TAKE INTO ACCOUNT EXACERBATING OR MITIGATING CIRCUMSTANCES. THESE RECOMMENDATIONS, EVEN IF CORRECTLY APPLIED, MAY CAUSE CONFLICTS IN THE OPERATING SYSTEM OR INSTALLED APPLICATIONS. ANY RECOMMENDED CHANGES TO THE OPERATING SYSTEM OR INSTALLED APPLICATION SHOULD FIRST BE EVALUATED IN A NON-PRODUCTION ENVIRONMENT BEFORE BEING DEPLOYED IN THE PRODUCTION ENVIRONMENT.

G' SECURE LABS

Recipient:

Name/role	Company
Deepak	Stryker

Document Version:

Name of the Author	Version	Title	Date
Arunesh Mishra	1.0	Planned list of Test Cases for Smart Medic Platform	April 12th, 2022

Table of Contents

1. Summary

Stryker has assigned the task of carrying out vulnerability assessment and penetration testing of their SmartMedic Platform by G'Secure Labs team. This is planned list of Test Cases for Smart Medic Platform. The version 1.0 detailed planned list of activities described about each validation process task.

2. Planned List of Test Cases

Test Case No.	Test Case Name	Test Case Steps	Test Case Performer	Test Case Result
GSL-STC-001	Malware Detection/Protection	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability	Arunesh Mishra	
GSL-STC-002	The Application shall support the use of anti-malware mechanism	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability	Arunesh Mishra	
GSL-STC-003	The Application shall have logs of tablet application and firmware (SmartMedic devices).	1) Check the logs of tablet application and firmware	Arunesh Mishra	
GSL-STC-004	The Application shall provide secure tunnel Communications channel	1) Use sniffing tool to sniff the data at motion and MITM 2) Check for the open ports 3) Exploit the open ports found while assessment and information gathering. 4) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 5) Exploit the found loopholes while VA scanning using kali tools.	Arunesh Mishra	
GSL-STC-005	The application shall allow to assign and edit patient reference ID to patient.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port	Arunesh Mishra	

		6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM		
GSL-STC-006	Security	1) Check the security settings of respective Smart Medic component	Arunesh Mishra	
GSL-STC-007	The Application shall establish technical controls to mitigate the potential for compromise to the integrity and confidentiality of health data stored on the product or removable media Since admin application shall be hosted as an independent azure web app and it shall have no open ports until there is explicit requirement.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-008	Application shall have the User Management Screen to configure and manage the users as per the roles.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the User Management Screen to configure and manage the users as per the roles	Arunesh Mishra	
GSL-STC-009	Invalid email or password, only 3 attempts left.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit and Brute Force attempt for the authentication/authorization on the open port	Arunesh Mishra	
GSL-STC-010	Only Stryker made/ authenticated devices should be able to communicate with SM device and tablet.	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device	Arunesh Mishra	

		4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM		
GSL-STC-011	Application shall use APIs to communicate between browser application and the backend.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-012	The Application shall have the 'Remember me' feature for login credentials and all the data which we shall store inside local storage shall be encrypted.	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability and encryption algorithm	Arunesh Mishra	
GSL-STC-013	System shall store patient id in anonymized fashion.	1) Exploit the devices with respect to vulnerability and anonymized algorithm	Arunesh Mishra	
GSL-STC-014	Invalid hospital code, only 3 attempts left.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit and Brute Force attempt for the authentication/authorization on the open port	Arunesh Mishra	

GSL-STC-015	Something went wrong with API operation try again / contact API admin.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-016	Transmission confidentiality and integrity	Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-017	Access control policy and management	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability and encryption algorithm	Arunesh Mishra	
GSL-STC-018	Generic messages should be displayed upon validation of credentials to mitigate the risk of account harvesting and enumeration.	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-019	The Application shall provide facility of audit logs for storing the user activity details.	1) Check the logs of tablet application and firmware related to user activity details.	Arunesh Mishra	
GSL-STC-020	Azure Cloud Infrastructure	8) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application.	Arunesh Mishra	

		9) Check for the open ports using nmap, other kali tools 10) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 11) Exploit the open ports using kali tools. 12) Brute Force attempt for the authentication/authorization on the open port 13) Exploit related to Brute Force attempt for the authentication/authorization on the open port 14) Use sniffing tool to sniff the data at motion and MITM		
GSL-STC-021	Nurse Station Web Services	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools. 5) Brute Force attempt for the authentication/authorization on the open port 6) Exploit related to Brute Force attempt for the authentication/authorization on the open port 7) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-022	The application shall allow to upgrade the tablet application.	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the upgradation process of the tablet application.	Arunesh Mishra	
GSL-STC-023	Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name	1) Brute Force attempt for the authentication/authorization on the open port 2) Exploit related to Brute Force attempt for the authentication/authorization on the open port	Arunesh Mishra	
GSL-STC-024	If the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools.	Arunesh Mishra	

		4) Exploit the open ports using kali tools.		
GSL-STC-025	The Application shall be validated by using invisible captcha during login	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.	Arunesh Mishra	
GSL-STC-026	TCP/IP Communication	Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-027	Cosmos DB	1) Vulnerability Assessment scanning for the identifying unknown vulnerabilities of web application. 2) Check for the open ports using nmap, other kali tools 3) Exploit the found loopholes while VA Scanning using the Burpsuite, kali tools. 4) Exploit the open ports using kali tools.	Arunesh Mishra	
GSL-STC-028	Currently, no such tool is being used	NA	Arunesh Mishra	
GSL-STC-029	Installation & Service Manual	NA	Arunesh Mishra	
GSL-STC-030	IOT Provisioning	1) Create Android malware 2) Transfer the malware to tablet/Smart Medic Device 3) Malware execution on the device 4) Exploit the devices with respect to vulnerability 5) Check for the open ports 6) Exploit the open ports found while assessment and information gathering. 7) Vulnerability Assessment scanning for the identifying unknown vulnerabilities 8) Exploit the found loopholes while VA scanning using kali tools. 9) Use sniffing tool to sniff the data at motion and MITM	Arunesh Mishra	
GSL-STC-031	Audit logs	1) Check the logs of tablet application and firmware related to user activity details.	Arunesh Mishra	
GSL-STC-032	Configuration settings	1) Check the security configuration settings	Arunesh Mishra	
GSL-STC-033	Future release	NA	Arunesh Mishra	

*** End of the document

G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES

THE NETHERLAND
Maria Montessorilaan 3,
2719 DB Zoetermeer,
The Netherlands

INDIA
B/81, Corporate House,
Judges Bungalow Road, Bodakdev,
Ahmedabad - 380054. India

www.gsecurelabs.com

Confidentiality Clause:

This document and any files with it are for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please destroy all copies of the document. Any unauthorized review, use, disclosure, dissemination, forwarding, printing or copying of this document or any action taken in reliance on this document is strictly prohibited and may be unlawful.